EXHIBIT 9

AO 106 (SDNY Rev. 01/17) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Southern District of New York

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
(1) the Forensic Image of an Apple iPhone 11 Pro Max, IMEI Number [redacted] created on or about November 15, 2019;
(2) the Forensic Image of an Apple iPhone 6s, IMEI Number [redacted], created on or about November 15, 2019; and
(3) a Seagate Hard Drive, Serial Number [redacted]

Case No. 19MAG11706

APPLICATION FOR A SEARCH AND SEIZURE WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

(1) the Forensic Image of an Apple iPhone 11 Pro Max, IMEI Number 353959100775675, created on or about November 15, 2019; (2) the Forensic Image of an Apple iPhone 6s, IMEI Number 353264079483991, created on or about November 15, 2019; and (3) a Seagate Hard Drive, Serial Number WL1B8AQ25

located in the Southern District of New York, there is now concealed *(identify the person or describe the property to be seized)*:

See Attached Affidavit and its Attachment A

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

X ❒ evidence of a crime;

❒ contraband, fruits of crime, or other items illegally possessed;

❒ property designed for use, intended for use, or used in committing a crime;

❒ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section(s)	*Offense Description(s)*
31 USC 5322	Bank Secrecy Act violations
50 USC 1701	Sanctions violations under International Emergency Economic Powers Act
18 USC 1519	Obstruction of justice

The application is based on these facts:

See Attached Affidavit and its Attachment A

☑ Continued on the attached sheet.

❒ Delayed notice of ____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Special Agent Elizabeth A. Kudirka, FBI
Printed name and title

Sworn to before me and signed in my presence.

Date: 12/13/2019

Judge's signature

City and state: New York, NY

U.S. Magistrate Judge Sarah L. Cave
Printed name and title

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

19MAG11706

In the Matter of the Application of the United States Of America for a Search and Seizure Warrant for:

(1) the Forensic Image of an Apple iPhone 11 Pro Max, IMEI Number [redacted], created on or about November 15, 2019;

(2) the Forensic Image of an Apple iPhone 6s, IMEI Number [redacted], created on or about November 15, 2019; and

(3) a Seagate Hard Drive, Serial Number [redacted]

(collectively, the "Subject Data").

TO BE FILED UNDER SEAL

Agent Affidavit in Support of Application for Search and Seizure Warrant

SOUTHERN DISTRICT OF NEW YORK) ss.:

ELIZABETH A. KUDIRKA, being duly sworn, deposes and says:

I. Introduction

A. Affiant

1. I am an "investigative or law enforcement officer" of the United States within the meaning of 18 U.S.C. § 2510(7), in that I am a sworn officer of the United States empowered by law to conduct criminal investigations and make arrests for offenses enumerated by 18 U.S.C. § 2516. I have been employed as a Special Agent of the Federal Bureau of Investigation ("FBI") since May 2018. Prior to becoming a Special Agent, I was an Investigative Specialist for the FBI, where I conducted surveillance operations in furtherance of counter terrorism, counterintelligence, criminal, and cyber investigations for three years. As a Special Agent, I attended a 20-week basic field training course where I received extensive training in law, investigative techniques, surveillance, tactics, and firearms. During that course, I received blocks of instruction on complex

financial crimes including money laundering and securities fraud. I have also completed FBI web-based instructional courses on complex financial crimes. I have examined digital evidence related to financial crimes cases, conducted numerous interviews of witnesses and victims, worked with several confidential human sources, participated in the execution of multiple search warrants and arrest warrants, monitored Title III wires and reviewed financial records.

2. I make this Affidavit in support of an application pursuant to Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the forensic images and electronic device specified below (the "Subject Data") for the items and information described in Attachment A. This affidavit is based upon my personal knowledge; my review of documents and other evidence; my conversations with other law enforcement personnel; and my training, experience and advice received concerning the use of computers in criminal activity and the forensic analysis of electronically stored information ("ESI"). Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts that I have learned during the course of my investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

B. The Subject Data

3. The Subject Data are particularly described as:

a. the Forensic Image of an Apple iPhone 11 Pro Max, IMEI Number [redacted], created on or about November 15, 2019 ("Forensic Image-1" and "Subject Device-1," respectively);

b. the Forensic Image of an Apple iPhone 6s, IMEI Number [redacted], created on or about November 15, 2019 ("Forensic Image-2" and "Subject Device-2," respectively); and

c. a Seagate Hard Drive, Serial Number [redacted] ("Subject Device-3")

(collectively, the "Subject Data").

4. Based on my training, experience, and research, and from consulting the manufacturer's advertisements and product technical specifications available online at https://support.apple.com/en_US/specs/iphone, I know that Subject Device-1 and Subject Device-2 (from which Forensic Image-1 and Forensic Image-2 were made) have capabilities that allow them to serve as wireless telephones, digital cameras, portable media players, GPS navigation devices, and PDAs.

5. Based on my training, experience, and research, I further know that Subject Device-3 is a hard drive that is used to store electronic data.

6. The Subject Data are presently located in the Southern District of New York.

C. The Subject Offenses

7. For the reasons detailed below, I believe that there is probable cause to believe that the Subject Data contain evidence of violations of Title 31, United States Code, Section 5322 (Bank Secrecy Act violations involving inadequate controls, recordkeeping, and reporting), Title 50, United States Code, Section 1701 (violations of the International Emergency Economic Powers Act based on sanctions violations), and Title 18, United States Code, Section 1519 (obstruction of justice).

II. Probable Cause

A. Probable Cause Regarding Subjects' Commission of the Subject Offenses

Background of the Investigation

8. Based on my participation in this investigation, I know that since in or about July 2019, the FBI has been investigating an online exchange called "BitMEX" and certain of its current and former employees for committing or causing violations of the Bank Secrecy Act ("BSA") and

the International Emergency Economic Powers Act ("IEEPA"). The FBI is also investigating obstruction of justice by a former BitMEX employee.

9. BitMEX (or the Bitcoin Mercantile Exchange) is a cryptocurrency exchange and derivative trading platform. BitMEX is owned and operated by "HDR Global Trading Limited," which is incorporated in the Seychelles and has a number of subsidiaries and affiliates registered in China, the United States, and elsewhere.

10. From my involvement in this investigation, and as set forth in more detail below, I submit that probable cause exists to believe that, since at least in or about 2014 and continuing through the present, BitMEX has operated within the United States, and/or has sold or offered to sell futures contracts to customers in the United States, and is therefore required to register as a Futures Commission Merchant ("FCM") with the U.S. Commodity Futures Trading Commission ("CFTC"), *see, e.g.*, 7 U.S.C. § 6d(a); *id.* § 1a(28)(A)(i)(aa)(AA); (2) because BitMEX is required to register with the CFTC (although it has never so registered), BitMEX is subject to the BSA, *see* 31 U.S.C. § 312(c)(1)(A); and (3) BitMEX and certain of its current and former employees have willfully violated and/or willfully caused BitMEX to violate the BSA's controls, reporting, and recordkeeping requirements by, among other things, failing to adopt adequate controls for accountholder verification, anti-money laundering, and anti-terrorist financing.

11. Respecting IEEPA, the investigation concerns certain transactions that BitMEX—which is majority beneficially owned by two U.S. citizens—engaged in with customers located in Iran, in violation of U.S. sanctions.

12. Finally, in the course of this investigation, the FBI has identified evidence that a former BitMEX employee obstructed justice by destroying relevant evidence before voluntarily meeting with the FBI and attorneys for the Government.

2019, the Bitcoin earned by BitMEX from the 434 identified U.S. users was worth approximately $1,340,289.71 USD.

BitMEX is Not CFTC Registered and Lacks Adequate Controls

15. Based on my review of the transcript of a deposition that the CFTC took of Arthur Hayes in or about July 2019 (the "Hayes Deposition"), I have learned, among other facts, that neither BitMEX nor any of its affiliated entities have ever applied to become registered in any capacity with the CFTC.

16. Based on my training and experience in prior investigations, and my review of the Internet Archive website (https://archive.org/), I have learned, among other facts, that the Internet Archive is an online library that includes, among other things, archived versions of websites. If a website has been captured by the Internet Archive on a particular date, the version of the website that was in existence on that date is preserved and can be viewed by the public. Not all websites are captured by the Internet Archive, and even websites that are captured may only have one snapshot taken or may have multiple snapshots spanning years of time.

17. Based on my review of archived versions of the registration page of the BitMEX website (https://www.bitmex.com/register) available on the Internet Archive, I have learned, among other facts that:

a. As of on or about March 16, 2015, BitMEX advertised the fact that "No real-name or other advanced verification is required on BitMEX." Some time between on or about March 6, 2015 and on or about November 21, 2015, that language was removed from BitMEX's registration page. In addition, a dropdown box for "Country of residence" was added.

b. Also as of on or about March 16, 2015, the registration page on the BitMEX website allowed customers to register on the platform by providing a username, email address, and

password. Customers were given the option to provide a first name and last name, but the BitMEX registration page explained that first and last name were "not required" to register and were "used for verification purposes if you lose your two-factor authentication" for account login. The BitMEX registration page continued to expressly state that first and last name were not required through at least on or about June 1, 2016. Some time between on or about June 1, 2016 and the version of the website available on or about January 16, 2017, this language was removed. As of on or about January 16, 2017, and continuing through the present, the BitMEX registration page has had asterisks next to the fields for entering a user's email address, password, and country (or region) of residence, but no asterisks appear next to the fields for first and last name. Based on my prior experience with websites and electronic forms, I understand that asterisks are typically used to denote mandatory fields, such that the lack of an asterisk next to the first and last name fields on the BitMEX registration page indicates that those fields were not and are not mandatory.

18. Based on my review of the transcript of a deposition that the CFTC took of Greg Dwyer in or about April 2019 (the "Dwyer Deposition"), I have learned the following facts, among others:

a. Dwyer began working at BitMEX in late 2015. He was the first employee of BitMEX aside from its three co-founders: Arthur Hayes, Sam Reed, and Ben Delo. Dwyer started with BitMEX as the head of business development has during his tenure also supervised customer support. Until the beginning of 2019, Dwyer worked for BitMEX from New York. Before joining BitMEX, Dwyer worked and shared an apartment with Hayes.

b. From the time that Dwyer joined BitMEX in or about 2015 through the date of his CFTC deposition in or about April 2019, BitMEX did not collect know-your-customer documents when individuals registered for BitMEX accounts and only took steps to verify

customer identification if an account was compromised or lost access.[1] As Dwyer described, a customer only needs a first name and last name, an email address, and a password to register for BitMEX, but BitMEX does not take steps upon signup to check the first and last name provided against any form of identification. Based on the information described in paragraph 17 above, Dwyer appears to be mistaken about the fact that BitMEX users needed a first and last name to register with the platform.

19. In or about November 2019, I interviewed a former BitMEX employee ("Witness-1")[2]. During those interviews, Witness-1 stated the following, in substance and in part:

a. Witness-1 is a former employee of BitMEX. In Witness-1's role at BitMEX, Witness-1 was familiar [redacted]

b. During Witness-1's tenure at BitMEX, BitMEX did not have formal know your customer verification upon customer registration and only attempted to verify accountholder

[1] When asked about know your customer policies during the Hayes Deposition, Hayes claimed that BitMEX has "risk-based" know-your-customer policies and procedures in which "certain actions by users or customers will trigger [BitMEX] to ask for additional information before they are allowed to continue[] operating on the platform." Hayes claimed that these risk-based policies are triggered in three specific circumstances: (1) if a customer is flagged as coming from a restricted jurisdiction and challenges that designation; (2) if a customer loses their two-factor authentication code; and (3) if one of the BitMEX founders in reviewing customer withdrawal activity notices "something out of place." Hayes acknowledged that this process did not apply to all customer accounts and nowhere claimed that BitMEX collected or verified accountholder identification across its customer base – data that would seem to be necessary to the assessment of risk associated with a particular customer in a "risk-based" KYC program.

[2] Witness-1 is cooperating with the Government's investigation [redacted] Further, and as described in more detail below, Witness-1 may face criminal exposure for obstruction; no promises regarding leniency as to any potential charges have been extended to Witness-1.

identification in limited situations such as when a customer lost their two-factor authentication or for email changes; BitMEX did not have anti-money laundering policies or controls; BitMEX did not file suspicious activity reports (or "SARS") with the U.S. government; and BitMEX did not have policies or procedures for identifying transactions subject to U.S. sanctions.

Iranian Customers and OFAC Self-Disclosure

20. Based on my review of records provided by BitMEX in response to a grand jury subpoena, I have learned, among other facts, that on or about September 19, 2019, BitMEX made a self-disclosure to OFAC of "potential apparent violations" of U.S. sanctions based on BitMEX's identification of "a number of account-holders that may have accessed the exchange from Iran." The letter further stated that BitMEX is majority beneficially owned by U.S. persons.

21. Based on my review of an electronic chat that was obtained from BitMEX pursuant to a grand jury subpoena, I have learned, among other facts, that in or November 2018, BitMEX co-founder Ben Delo had a conversation with another BitMEX employee regarding the existing IP controls at BitMEX and explaining, in substance and in part, that a revised approach would have the benefit of "strict enforcement of US sanctions against Iran etc." because the IP geolocation data used by BitMEX "is stale (from 2 months ago)" such that BitMEX "currently let[s] these people [*i.e.*, customers operating from Iranian IP addresses] slip through the cracks."

Witness-1's Destruction of Evidence

22. Based on my participation in interviews of Witness-1, I have learned, among other facts, that in the days prior to Witness-1 meeting with the FBI and attorneys for the Government, Witness-1 deleted information from Subject Device-1 and Subject Device-2 relating to Witness-1's employment at BitMEX and BitMEX's operations, including evidence of BitMEX having U.S. customers.

23. Based on my participation in interviews of Witness-1, I have learned, among other facts, that in the days prior to Witness-1 meeting with the FBI and attorneys for the Government, Witness-1 directed a third party to destroy Subject Device-3, a hard drive that contained certain data that Witness-1 had saved from Witness-1's corporate laptop while an employee at BitMEX. This data included files that [redacted] and that evidenced, among other things, that BitMEX had transacted with persons in the United States and Iran. According to Witness-1, Subject Device-3 also included other materials [redacted] that related to BitMEX's operations, including its trading practices and failures of know-your-customer protocols.

B. Probable Cause Justifying Search of the Subject Data

24. Based on my participation in interviews of Witness-1 in or about November 2019, I have learned the following facts, among others:

a. Witness-1 stored information concerning Witness-1's employment at BitMEX on Subject Device-1 and Subject Device-2, including information that Witness-1 deleted or attempted to delete in the days prior to Witness-1 meeting with the FBI and attorneys for the Government, and other information that remained on Subject Device-1 and Subject Device-2.

b. For example, Witness-1 described using Witness-1's cellphones to communicate with other employees at BitMEX and taking photographs of BitMEX's office space, BitMEX events, and BitMEX corporate documents using those cellphones. Witness-1 showed me examples of certain saved copies of these photographs and described additional screenshots that Witness-1 had deleted from Subject Device-1 and Subject Device-2, including evidence of U.S. customers on the BitMEX platform.

c. Witness-1 used a Cloud-based program to save and access data on Subject Device-1 and Subject Device-2, so that materials to which Witness-1 had access on one device was also accessible to Witness-1 on the other device.

d. Witness-1 also stored information relating to BitMEX's operations, including its transactions with persons located in the United States and Iran, on Subject Device-3. For example, Witness-1 stated that the types of information that Witness-1 would have saved to Witness-1's BitMEX laptop and backed up to Subject Device-3 would include, among other types of materials, screenshots of information that Witness-1 used in Witness-1's work at BitMEX, information concerning customer withdrawals, and customer support tickets.

e. In the days prior to Witness-1 meeting with the FBI and attorneys for the Government, Witness-1 directed a third party to destroy Subject Device-3. At the FBI's instruction, during my meetings with Witness-1 in or about November 2019, Witness-1 directed that same third party to mail Subject Device-3 to the FBI. The FBI received Subject Device-3 by mail on or about December 4, 2019. I have seen Subject Device-3 in its current condition, and based on my observations and training and experience, the connectors used to plug the drive into a computer appear damaged but the drive is otherwise intact and the data contained thereon is likely recoverable.

f. As noted in paragraph 17(a) above, Witness-1 is a former employee of BitMEX. In Witness-1's role at BitMEX, Witness-1 was familiar with [redacted]. Witness-1 was first in communication with employees of BitMEX beginning in or about [redacted] and has been in contact with BitMEX employees and/or customers throughout [redacted]